GIBSON, DUNN & CRUTCHER LLP
Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Rosemarie T. Ring (SBN 220769)
rring@gibsondunn.com
Austin V. Schwing (SBN 211696)
aschwing@gibsondunn.com
Martie Kutscher (SBN 302650)
mkutscherclark@gibsondunn.com
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

GIBSON, DUNN & CRUTCHER LLP
Deborah Stein (SBN 224570)
dstein@gibsondunn.com
Heather L. Richardson (SBN 246517)
hrichardson@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Attorneys for Defendant Facebook, Inc.,

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

DECLARATION OF ELIZABETH DUNPHY IN SUPPORT OF SETTLEMENT

I, Elizabeth Dunphy, hereby declare and state as follows, to the best of my knowledge, information, and belief:

1. I am a Director of Privacy Compliance Management at Meta Platforms, Inc., formerly known as Facebook, Inc. ("Meta"). I offer this declaration regarding Meta's oversight of third-party developers' access to and use of data regarding the Users of Meta's Facebook product.[1] I have personal knowledge of the facts set forth in this declaration, and, if called to testify, I could and would competently testify to them.

2. As explained below, Meta employs a multilayered approach to overseeing and managing developers' access to data regarding Facebook Users. This approach includes reviewing developers' requests for access to data, periodically re-reviewing developers' access to data, and ongoing monitoring of such access.

A. Privacy Review.

3. Meta maintains a privacy review process ("Privacy Review"), which ensures that privacy is an integral part of designing innovative new products and features, ideally in the early stages of development. It also provides broad visibility for key cross-functional stakeholders into risk

[1] In this declaration, "developer" refers to a party whose product facilitates the use of Covered Information in an independent, third-party consumer app or website. These parties are also referred to as "E.1 Covered Third Parties," in reference to the developers described in Section VII.E.1 of the Decision and Order in *In re Facebook, Inc.*, FTC File No. 182-3109, C-4365 (F.T.C. April 28, 2020) ("FTC Order"). "Covered Information" means information from or about an individual consumer including, but not limited to: (a) a first or last name; (b) geolocation information sufficient to identify a street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging User identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID, or other persistent identifier that can be used to recognize a User over time and across different devices, websites or online services; (g) a Social Security number; (h) a driver's license or other government issued identification number; (i) financial account number; (j) credit or debit information; (k) date of birth; (l) biometric information; (m) any information combined with any of (a) through (l) above; or (n) Nonpublic User Information. "Nonpublic User Information" means any User profile information (i.e., information that a User adds to or is listed on a User's Facebook profile), or User-generated content (e.g., status updates, photos), that is restricted by one or more Privacy Settings. "Privacy Setting" includes any control or setting provided by Meta that allows a User to restrict which individuals or entities can access or view Covered Information. "User" means an identified individual from whom Meta has obtained information for the purpose of providing access to its products and services.

mitigation across the company's products and services. Privacy Review evaluates new or modified products, services, or practices (together, "Projects") that involve the collection, use, or sharing of User data to assess privacy risks and recommends safeguards to mitigate those risks. Privacy Review is a prerequisite to launch Projects that collect or share new User data, use User data in a new way, or involve statements about the extent to which Facebook maintains the privacy and security of User data.

4. At a high level, Privacy Review includes the following "privacy by design" processes and activities, among others:

a. **Project Guidance.** The owner of the Project ("Project Owner") liaises with their privacy cross-functional ("PXFN") team for guidance on how to anticipate and minimize privacy risks throughout Project design.

b. **Project Intake.** To initiate a Privacy Review, the Project Owner completes an intake form. The standard product intake form in Launch Manager includes questions relating to data collection, data sharing, data use, notice and consent, safeguards and risks, and mitigations.

c. **Project Review.** A PXFN team will be designated to review the Project information. During the review process, the PXFN team works to identify potential risks to the privacy, confidentiality, or integrity of User data and to identify mitigations to minimize those risks.

d. **Privacy Decision.** The PXFN reviewers sign off on the Privacy Decision in Launch Manager, which indicates whether the Project was approved, approved pending Implementation Review, rejected, or closed.

5. Among other things, Meta leverages Privacy Review to ensure that it provides Users with appropriate notice and obtains affirmative express consent where required. Launch Manager requires information about User disclosures and consent and documents those findings.

6. The current version of the Privacy Review process was implemented at scale in October 2020, and subsequently has been refined.

B. Initial Review of Third-Party Access to Covered Information.

7. When a developer requests access to Covered Information other than public profile information and email through a Public API[2] for use in an independent third-party consumer application or website ("App"), Meta conditions access through a process called App Review.

a. In App Review, a team of Developer Operations ("DevOps") reviewers evaluates the App's use of the Covered Information against the permissible use cases for such information and the developer's compliance with Meta's Platform Terms and Developer Policies and decides whether to approve or deny the request for access to Covered Information.

b. This process is designed to ensure that developers have a legitimate and permissible reason for obtaining Covered Information through Meta's API products and that the privacy policies of Apps developers have submitted for approval are in compliance with Platform Terms.

c. The App Review process was implemented in 2014, and subsequently has been refined.

8. In some cases, developers utilize Partner APIs, which are APIs made available on an individual partner basis. When a developer requests access to a Partner API for use in an independent third-party consumer application or website, Meta conditions access through the Partner Grant Review process.

a. This process is managed by Meta's Partnerships team. It involves sets of standard questions designed to help the reviewer evaluate the App's use of the Covered Information and the developer's compliance with Meta's Platform Terms.

b. Like App Review, the Partner Grant Review process involves verification that developers have functional links to their privacy policies in their Apps.

c. The Partner Grant Review process was implemented in February 2019.

[2] "Application Programming Interface." Public APIs are the set of APIs for which access can be requested by any developer on Facebook's developer platform.

9. Meta additionally uses verification processes to help validate that developers are not misrepresenting their identity prior to receiving access to certain categories of Covered Information by requiring evidence from developers to confirm their represented identities.

C. Periodic Reassessment.

10. At least once every twelve months, Meta conducts assessments and operational testing of all developer Apps with access to Covered Information through one or more Public API products to identify violations or potential violations of Platform Terms in a process known as App Re-Review.

11. While Meta refers to this process as App Re-Review, it is distinct from Meta's separate App Review process in both scope and cadence. App Re-Review applies to a larger population of Apps than App Review, including those that access only public profile information and email. In addition, App Re-Review occurs at least annually, and not based on when the App went through App Review.

a. In App Re-Review, Meta, through a team of DevOps reviewers, assesses each App using a set of standard questions designed to identify potential violations of Platform Terms. For example, for an App that obtains data through the "user_hometown" permission, the App Re-Reviewer would assess whether the App "provide[s] a personalized experience based on where a person lived or grew up," consistent with the allowed usages for that permission.

b. Among others, Meta uses the following questions for App Re-Review reviewers to investigate regarding subject Apps:

- Does the privacy policy lack a clear explanation of what data the App is collecting about the user?
- Does the privacy policy lack a clear explanation of what purposes the App is using that data?
- Does the privacy policy lack a clear explanation of how the user may request that the data be deleted?
- Does the App appear to use Meta data to make eligibility determinations about people (determining whether to provide, deny, or take away a particular benefit as well as determining the terms under which the benefit will be provided, denied, or taken away), including for housing,

employment, insurance, education opportunities, credit, government benefits, or immigration status.

- Does the App appear to use Meta data to make decisions based on people's race, ethnicity, color, national origin, religion, age, sex, sexual orientation, gender identity, family status, disability, medical or genetic condition?[3]
- Does the App appear to use Meta data for activities related to surveillance?

If the answer to any of these questions is in the affirmative, the App Re-Reviewer will refer the App to the DevOps Enforcement team for enforcement.

c. The App Re-Review process also involves rigorous operational testing of all developer Apps that access at least one Public API product. Specifically, this process requires reviewers to directly engage with each App's functionality—through hands-on testing, developer-led live walkthroughs, or reviews of screencasts—to identify, among other things, potential violations of applicable Platform Terms.

d. Meta implemented the modified processes described in Paragraphs 11(a)-(c) for Facebook Platform App Re-Reviews on or about September 7, 2021.

12. Meta also annually evaluates Apps that access Covered Information through Partner APIs through the Partner Grant Re-Review process.

a. Like the initial Partner Grant Review, this process is managed by Meta's Partnerships team and involves sets of standard questions designed to help the reviewer evaluate the App's use of the Covered Information and the developer's compliance with Meta's Platform Terms.

b. This process includes technical and operational testing of Apps' compliance with the Platform Terms.

c. As with annual App Re-Review, Meta has also enhanced its Partner Re-Review process so that reviewers now assess not only whether the privacy policy link is functional but also whether the policy appearing at the link explains what data the App processes, the purposes

[3] Section 3(a)(i) of Meta's Platform Terms prohibits discrimination on the basis of these factors. Certain Apps, such as dating Apps that consider Users' sex and sexual orientation, are permitted under the Platform Terms to make decisions on the basis of these factors.

for which the App processes the data, and how Users may request deletion of the data maintained by the developer.

d. Meta implemented the modified processes described in Paragraphs 12(a)-(c) for Facebook Platform Partner Grant Re-Reviews on or about September 7, 2021.

13. As yet another annual process, Meta requires developers to annually (i) certify continued compliance with applicable Meta terms, and (ii) certify that each one of their purpose(s) or use(s) for Covered Information complies with Meta's permissible purpose(s) or uses(s) for that type of Covered Information in order to maintain access to permissions, capabilities, and/or features associated with E.1 API products.

a. Meta obtains such self-certifications on a per-App basis through the Data Use Checkup tool ("DUC"). Through DUC, Meta requires an administrator registered with each App of an E.1 Covered Third Party to certify compliance with Platform Terms and how they use the Covered Information to which they have access. In particular, DUC presents the administrator with a list of individual integrations (e.g., Public APIs and Partner APIs that enable the App to access Covered Information).

b. For each integration, DUC requires the administrator to confirm that the App's use of the integration complies with the allowed usage for the data available through that API. DUC also requires the administrator to confirm that the App complies with Platform Terms. The administrator cannot submit an incomplete certification (although they may elect to remove integrations to which they no longer wish to have access, thereby preventing the App from accessing the corresponding data).

c. Meta maintains an automated process to notify the administrator associated with each applicable App of the administrator's obligation to complete the DUC. Meta issues these notices such that each E.1 Covered Third Party is required to certify for its covered Apps at least annually. Meta requires E.1 Covered Third Parties with multiple covered Apps to complete DUC for each of their Apps.

d. Once Meta sends a request to a third party to complete an annual self-certification, Meta provides the third party 60 days to complete the self-certification. If an administrator fails to complete the DUC within 60 days, Meta initiates an automated process through which it progressively reduces the App's access to Facebook's APIs over the course of 30 days, at the end of which Meta blocks the App's access to Facebook APIs altogether. If the administrator completes the App's self-certification, Meta restores the App's access.

e. Meta implemented the DUC in 2020.

D. Risk-Based Assessments.

14. In addition to initial and periodic assessments, Meta performs additional review of data use by Apps in higher-risk tiers.

15. Meta has developed a framework to assign any given E.1 Covered Third Party App to one of five risk tiers (Tier A though Tier E, with Tier A carrying the least risk) based on two separate evaluations of risk: (i) an evaluation of the risks inherent to the API products used by the App (the "Product Risk Assessment") and (ii) an evaluation of risk characteristics specific to the App itself (for example, volume of Users) (the "Third Party Risk Assessment"). This framework is operationalized to apply on an ongoing basis through an automated process that formally applies the framework daily to each E.1 Covered Third Party App.

a. The Product Risk Assessment assesses the degree of risk posed by the API product(s) to which any given E.1 Covered Third Party App has access. During this "Product Risk Assessment," Meta assigns each E.1 Covered Third Party App a "Product Risk Tier" designation based on the E.1 API product(s) to which the App has access. Meta's Privacy, Platform, Product, and Legal organizations have assigned a risk tier, labeled from Tier A through Tier D in increasing order of relative risk, to each of Meta's E.1 API products that provide access to Covered Information. That assignment is based on the following risk factors:

- <u>Data Type Risk.</u> This factor examines risks related to the sensitivity of the specific Covered Information being shared through the E.1 API product, along with the User's and the third party developer's relationship to that Covered Information. Examples of Data Type Risk considerations are: whether such information is publicly available, whether the third party would have access to such information independent of its use of the E.1 API product, whether such information was generated by the User on

Facebook surfaces (e.g., Likes and Posts), whether the data is of a "social" nature (e.g., a list of friends), and whether the data is understood to be particularly sensitive (e.g., health or financial information).

- Consent & User Involvement. This factor considers the circumstances in which the User provides data to E.1 Covered Third Parties through a product, including the extent of their direction or other involvement in the sharing of the data through the product. For one, this factor considers whether the User has expressly consented to the sharing and can revoke the sharing at will. Meta's oEmbed API product, for example, only provides developers access to publicly available Facebook content, and thus does not rely on express, App-specific User consent. This factor also considers whether the User would have provided the information to the E.1 Covered Third Party regardless of that third party's Meta product integration. For example, the sharing of email addresses with Covered Third Parties is facilitated by the Facebook Login product, but that sharing takes place in the specific circumstance of account creation in which Users would otherwise share that same data directly with the third party without any involvement of Meta products.

- Volume of Accessible Covered Information. This factor looks at the anticipated volume of Covered Information that an E.1 Covered Third Party would collect from an API product, as determined based on the number of data elements shared and whether the data is static or dynamic (i.e., whether the data needs to be updated or augmented frequently through API calls). For example, where a product permits access to relatively static Covered Information (e.g., name, email, birthdate, or gender), the relative volume of Covered Information collected through the product is lower because the E.1 Covered Third Parties generally only need to obtain the information from the User once. By contrast, where a product permits access to a dynamic set of Covered Information (e.g., photos or likes), the volume of new Covered Information a E.1 Covered Third Party may access per User is relatively higher (as Users may add or update photos relatively often) and may increase over time as the E1 Covered Third Party requests this data from Meta to ensure it has up-to-date data for the service it provides to the User.

- Product Risk of Misuse. This is a factor that accounts for any other circumstances related to the data sharing that create or mitigate specific risks related to privacy, confidentiality, or Integrity of Covered Information. For example, where an API product includes sharing of a User's phone number, Meta treats such sharing as higher risk based on the understanding that phone numbers may be more likely to be abused to facilitate fraud or spam.

b. The risk factors described above are used to determine the Product Risk Tier for any E.1 Covered Third Party App with access to that product. In other words, if an E.1 Covered Third Party App has access to an API product that has been designated Tier C, then that App is assigned a Product Risk Tier C. If a single E.1 Covered Third Party App has access to Covered Information through multiple E.1 API products, the highest-risk product determines the App's product-level risk designation. For example, if an App has access to both a Tier A and a Tier D API product, then that App would have a Product Risk Tier designation of Tier D.

c. In addition to the Product Risk Assessment, Meta conducts an evaluation of risk factors specific to any given E.1 Covered Third Party App. This "Third Party Risk Assessment" results in a "Third Party Risk Tier" designation for each App. Meta currently determines the Third Party Risk Tier on the basis of two "risk signals"—i.e., characteristics of any given E.1 Covered Third Party App that Meta considers to be meaningfully correlated to risk relating to the privacy, confidentiality, and Integrity of Covered Information. First, Meta considers the total volume of active Users whose Covered Information is received by an App (the "Volume Signal"). Second, Meta considers the rate of User growth that an App has experienced (the "Growth Signal").

d. As previewed above, the Product Risk Assessment and Third Party Risk Assessment come together to determine the final E.1 Covered Third Party Risk Assessment tier assignment for any given E.1 Covered Third Party App. This final risk tier designation ranges from Tier A through Tier E, in increasing order of relative risk.

e. For Facebook E.1 Covered Third Party Apps, the Product Risk Assessment and the Third Party Risk Assessment are combined to generate the final E.1 Covered Third Party Risk Assessment tiers as indicated in the matrix below:

		Third Party Assessment			
	Tier	**A**	**B**	**C**	**D**
Product Assessment	**A**	A	A	A	A
	B	B	B	C	D
	C	B	C	D	E
	D	C	D	E	E

f. Meta initially completed its E.1 Covered Third Party Risk Assessment framework in August 2021, and continued to refine that framework through September 2021. On October 18, 2021, Meta implemented an automated process to apply the E.1 Covered Third Party Risk Assessment framework to all E.1 Covered Third Party Apps on a daily basis. Specifically, Meta's Developer Platform team maintains an automated process that executes at least once each day in order to identify the Product Risk Tier and Third Party Risk Tier for each E.1 Covered Third Party App, based on its product access and third party risk characteristics at that time, and to assign and record the App's final E.1 Covered Third Party Risk Assessment Tier as per the logic indicated in the matrices above.

g. Meta uses the E.1 Covered Third Party Risk Assessment tier designations to determine the appropriate level of monitoring processes to apply to any given E.1 Covered Third Party App. For example, a Tier E App will be subject to more rigorous monitoring processes than a Tier A App.

16. One such process that is required for Apps in Meta's four highest risk tiers (Tier B through E) is the Data Protection Assessment ("DPA"). These Apps must, at least once a year,

complete a questionnaire that collects information concerning the developer's adherence to Platform Terms. The questionnaire requires developers to answer multiple-choice questions, provide written responses, and submit documentary evidence regarding their App's data usage, data sharing, privacy policies, use of service providers, tech provider relationships, and data security.

a. The question set is dynamic; depending on how the developer answers certain questions, they may be prompted to answer additional questions. For example, if a developer indicates that it uses service providers, it will be prompted to answer questions about how it shares data with those service providers. The DPA is also designed to scale with the level of risk posed by any given App, meaning Apps in higher risk tiers go through a more rigorous assessment.

b. Once a completed questionnaire is received, the developer's answers are scored. For each question, Meta has identified answers and evidence that are acceptable; answers and evidence that are unacceptable and lead directly to enforcement for violation of the Platform Terms in accordance with the Enforcement Rubric; and answers and evidence that require follow-up investigation by reviewers before a violation of the Platform Terms can be confirmed. The E.1 Covered Third Party App "passes" the DPA only if all of the developer's answers and evidence are acceptable or, as applicable, a follow-up investigation confirms that the App is in compliance with the Platform Terms.

c. If a developer fails to respond, in full or in part, to the Data Protection Assessment within the time period allotted for a given E.1 Covered Third Party App, Meta will gradually throttle the App's API calls over the course of thirty days. If the developer has still not responded to the DPA at the end of the thirty-day throttling period, Meta will deactivate the subject App on the Facebook Developer Platform.

d. Meta began sending DPAs to developers on the Facebook Platform on or about August 9, 2021.

17. In connection with the DPA, Meta also engages in a process called Enhanced Privacy Policy Review.

a. The Enhanced Privacy Policy Review is a process by which Meta's DevOps team conducts a thorough assessment of each Tier E App's privacy policy at least once every twelve months in order to identify violations or potential violations of Platform Terms.

b. Specifically, the DevOps team conducts two targeted reviews. First, the DevOps team reviews each Tier E App's privacy policy to confirm whether the privacy policy is in compliance with applicable Platform Terms regarding the content of privacy policies. For example, for Tier E E.1 Covered Third Party Apps subject to the "Facebook Platform Terms" (available at https://developers.facebook.com/terms/dfc_platform_terms/), the DevOps team reviews for compliance with Section 4.b of those terms, which requires that privacy policies "accurately and clearly explain what data you are Processing, how you are Processing it, the purposes for which you are Processing it, and how Users may request deletion of that data." If any privacy policy is found to be in violation of Section 4.b, the DevOps team refers that App to the DevOps Enforcement team for enforcement on the basis of that violation.

c. Second, the DevOps team reviews each Tier E App's privacy policy to identify potential violations of certain other Platform Terms. For example, for Apps subject to the Facebook Platform Terms, the DevOps team reviews in order to identify potential violations of Section 3 of those terms, which concerns data use—including, for example, terms prohibiting unauthorized sharing of User data with fourth parties and requiring User data to be promptly deleted upon request or when no longer needed (among other circumstances). If the DevOps team suspects a violation of such terms, the DevOps team will refer the privacy policy to Meta's Legal team to conduct a secondary review to confirm whether there is a violation. If a policy violation is confirmed in the course of that review, the App will be further referred to the DevOps Enforcement team for enforcement on the basis of that violation.

d. Meta began conducting Enhanced Privacy Policy Reviews on or about August 16, 2021.

E. Monitoring.

18. Meta uses multiple automated processes to monitor third parties' use of User data.

19. The first of Meta's processes that provides ongoing monitoring of third parties is Meta's automated privacy policy scanning process.

a. Meta requires developers to provide links to their privacy policies in the dashboard on developers.facebook.com corresponding to their App.

b. Meta has developed a computer script that runs on a weekly basis that checks the privacy policy links of certain developers' Apps to confirm that Meta can successfully reach the webpage containing the privacy policy. More specifically, the script first compiles a list of any App that, within the last 90 days, has requested data from a Public or Partner API for use in an independent, third-party consumer application or website. For each of these Apps, the script attempts to open the webpage for the App's privacy policy.

c. This process has been implemented in its current form since on or about March 23, 2021.

20. Meta also makes use of automated rate limiting and automated removal of unused permissions and features processes to mitigate risks related to Meta's Platform Terms by mediating and/or limiting the volume and categories of Covered Information available to third party developers.

a. As part of automated rate limiting, Meta checks Apps to identify those that use a high volume of data and may limit the amount of data those applications can access.

b. As part of automated removal of unused permissions and features, Meta checks Apps for Public APIs that have not been used in 90 days and for any Partner APIs that have not been used in 30 days and revokes access to these APIs.

21. Meta additionally uses granular data permissions processes that are designed to ensure that Covered Third Parties are not able to access certain categories of Covered Information without prior and unrevoked consent from the User.

22. Meta also employs signals-based monitoring processes that are designed to collect and analyze information from various sources to identify potential Platform Terms violations. These signals, if indicative of a potential policy violation, may (1) trigger an Ad Hoc Review process, which can lead to a direct enforcement action or referral to a comprehensive investigation conducted by DevOps, or (2) be referred directly to DevOps to initiate an investigation.

a. Examples of the signals monitored include:

- Internal DevOps support forms, submitted by Meta employees who have reason to believe a third party is misusing data;
- External reporting forms for Facebook developers to report potential incidents implicating User data, such as a security breach;
- Data Abuse Bounty Program forms, submitted by third parties that have identified suspected misuse of Meta data;
- Public source leads (e.g., news articles about suspected data misuse);
- Reports from Meta's Global Threat Intelligence Monitoring team and Social Media Monitoring team, which proactively monitor for threats against Meta Users and the company's assets; and
- Reports from the External Data Misuse team, which maintains a process through which it retains security vendors to proactively search for public unsecured datasets and public brokered datasets and assess whether these datasets contain Meta data, which may be associated with a specific App or developer.

23. Finally, Meta mitigates Covered Third Party risks in the ordinary course by deprecating API products or by altering their design to limit data access or constrain appropriate use. As detailed in prior public statements, from 2014 to the present Meta has substantially reduced the number of data fields available to developers via Facebook Login. Examples of these product deprecations and restrictions include:

a. Beginning with an announcement at Meta's F8 developer conference in 2014, Meta has eliminated all 26 data fields through which a User could choose to share other Users' data (sometimes referred to as "friends data"). The user_friends data field, which remains active, allows a User to share a list of their own friends in very narrow contexts: only if (i) both the User and the friend have that App installed; and (ii) both friends have consented to sharing that information.

b. Similarly, in 2018, Meta deprecated several Facebook Login API features, including those that had provided access to religion, political views, and relationship details.

c. In addition, in 2019 Meta changed its Platform Policies to enable the removal of "quiz Apps" that provide minimal utility to Users relative to the risks involved with their access to sensitive User data. Meta also designed a process for limiting the data access of any remaining or subsequently identified minimum utility Apps on the platform.

F. Enforcement.

24. Over the years, Meta has dedicated significant and increasing resources to developing policies, monitoring third-party apps, and enforcing its policies. Meta has also continued to expand its monitoring and enforcement teams over the years.

a. The DevOps team, for example, grew significantly between 2013 and 2018, and it supplemented its enforcement efforts with individuals from other teams across the company (*e.g.*, Legal, Policy, Data Science, Engineering, Privacy).

b. By 2019, the DevOps team had grown to include approximately 90 full-time employees and close to 400 supporting vendors across the world.

c. By 2021, the DevOps team had grown to include more than 100 full-time employees and nearly 500 supporting vendors.

d. These personnel include cybersecurity experts and experienced law enforcement officers such as former federal prosecutors and FBI personnel, dedicated to safety and security.

e. All of these teams coordinate with each other, with Meta's Policy and Legal teams, and with Meta management more generally on enforcement efforts. Enforcement is a company-wide effort.

DATED: December 16, 2022

ELIZABETH DUNPHY